IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IRMA COLEMAN, et al.,

Plaintiffs,

-vs- **Case No. 17-cv-130-DRH**

ASTRAZENECA PHARMACEUTICALS, LP, et al.,

Defendants.

JOHN ROSENSTEEL, et al.,

Plaintiffs,

-vs- **Case No. 17-cv-131-DRH**

ASTRAZENECA PHARMACEUTICALS, LP, et al.,

Defendants.

NICHOLAS SKAGGS, II, et al.,

Plaintiffs,

-vs- **Case No. 17-cv-132-DRH**

ASTRAZENECA PHARMACEUTICALS, LP, et al.,

Defendants.

KENNETH LLOYD DRAVLAND, JR.

Plaintiff,

-vs- **Case No. 17-cv-133-DRH**

ASTRAZENECA PHARMACEUTICALS, LP, et al.,

Defendants.

ORDER REGARDING THE FORMAT OF PRODUCTION OF HARDCOPY DOCUMENTS AND ELECTRONICALLY STORED INFORMATION

The "Parties" (Plaintiffs and Defendants AstraZeneca LP, AstraZeneca Pharmaceuticals LP (collectively "AstraZeneca"), The Procter & Gamble Manufacturing Company; The Procter & Gamble Company (collectively "Procter & Gamble"), Wyeth Pharmaceuticals, Inc., Wyeth LLC (collectively "Wyeth"), and Pfizer, Inc., hereby agree to the following protocol for production of electronically stored information ("ESI") and paper ("hardcopy") documents (collectively "Documents") (the "Protocol" or "Discovery Order").[1] This Protocol, as well as any Protective Order entered by the Court, shall govern all production in the above-captioned matter, including any appeal therefrom and any other proton pump inhibitor litigation filed by undersigned counsel (collectively "the Litigation").[2] Nothing in this Protocol shall limit or waive a Party's right to seek or object to discovery as set out in applicable rules, to rely on any protective order entered in this action concerning protection of confidential or otherwise sensitive information, or to object to the relevance, admissibility or authenticity of any Document produced in accordance with this Protocol.

A. GENERAL AGREEMENTS

1. Ongoing Cooperation among the Parties

The Parties are aware of the importance the Court places on cooperation and commit to continue to consult and cooperate reasonably as discovery proceeds.

2. Preservation

[1] The Parties acknowledge that AstraZeneca has previously collected, processed and produced Documents in another litigation involving Nexium and Prilosec. AstraZeneca will produce previously produced Documents of interest (i.e. INDs, NDAs). The parties are currently conferring on other previously collected and/or produced Documents that will be re-produced in this Litigation. The Parties will meet and confer to determine the parameters of production to be applied to these Documents; however, AstraZeneca shall not be required or obligated to redo prior discovery to the extent there are differences with this Protocol.

[2] The Parties agree that no Documents will be produced until after a Protective Order is entered by the Court.

The Parties represent that pursuant to Federal Rule of Civil Procedure 26(b)(1), that they have taken reasonable and proportional steps to preserve reasonably accessible Documents that are relevant to the claims and defenses in the Litigation, including implementation of a litigation hold.

Activities undertaken by or at the direction of counsel in compliance with the duty to preserve information are protected from disclosure and discovery under the Federal Rule of Civil Procedure 26(b)(3).

3. Proportionality

In accordance with the Federal Rules, the Parties agree to seek discovery regarding any non-privileged matter that is relevant to any Party's claim or defense and proportional to the needs of the case. Identification of relevant Documents for collection and production shall occur through identification of appropriate Custodians and Non-Custodial Document Sources (as defined below) (collectively "Sources") and search parameters pursuant to meet and confer. The Parties will continue to consult and cooperate reasonably throughout discovery, to discuss, as appropriate, legitimate questions or issues (if any) that arise.

a. Non-Discoverable ESI. The Parties acknowledge that some ESI may be deemed inaccessible and not discoverable and 30(b)(6) depositions are being requested,. The Parties shall meet and confer on the extent to which the following categories of information may be non-discoverable.

i. Documents deleted in the normal course of business before the time a preservation obligation in this Litigation came into effect;

ii. Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of media, and that are substantially duplicative of data that are more accessible elsewhere;

iii. Deleted, "slack," fragmented, or unallocated data;

iv. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

v. On-line access data such as (without limitation) temporary internet files, history files, cache files, and cookies;

vi. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates;

vii. Electronic data (e.g., call logs, email, calendars, contact data, notes, and text messages) on or sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices);

viii. Voicemail not retained in the ordinary course of business;

ix. Instant messages not retained in the ordinary course of business;

x. Server, system, network or software application logs;

xi. Data remaining from systems no longer in use that are unreadable on the systems in use;

xii. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report.

xiii. Structural files not material to individual file contents that do not contain substantive content (e.g. .CSS, .XSL, .XML, .DTD, etc.).

b. Disaster-Recovery Backup Data. Absent a Party's specific written notice for good cause, no Party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes. Absent a showing of good cause, such backup media shall be considered to be not reasonably accessible.

4. No Designation of Discovery Requests

In accordance with Federal Rule of Civil Procedure 34(b)(2)(E)(i), the Producing Party shall produce Documents as they exist in the ordinary course of business and therefore shall not be required to organize or label productions to correspond to specific discovery requests. Any Custodial Files or Non-Custodial Document Sources (collectively "Sources") will be produced in the reasonably usable and searchable format as set forth herein, and each production will be accompanied by a production log, in native Excel spreadsheet format, identifying the Bates range of each production that corresponds to each Source.

Should the Requesting Party make a reasonable request for identification by Bates number of groups of Documents that the Producing Party can easily and readily

identify, the Producing Party shall cooperate and provide such information as soon as reasonably practicable considering the scope of the request and the volume of Documents implicated.

5. Sources

a. Defendants: Following service of Plaintiffs' Discovery Requests, Plaintiffs and counsel for each Defendant will meet and confer regarding the "Sources" (Custodians and Non-Custodial Document Sources) that contain information responsive to Plaintiffs Discovery Requests. Each Defendant will disclose to Plaintiffs the "Non-Custodial Document Sources" (those managed or accessed by multiple persons) and employees most likely to possess relevant Documents ("Custodians"), whose Custodial Files will be subject to collection and production. The Parties will continue to meet and confer regarding production of any additional Custodians and Non-Custodial Document Sources reasonably sought by Plaintiffs to ensure discovery is reasonable and proportional. Each Defendant will produce to Plaintiffs relevant, non-privileged Documents from Non-Custodial Document Sources or the individuals' Custodial Files.

i. AstraZeneca defines "Custodial File" to include: Documents maintained in the Custodian's hard copy files; Documents maintained on the Custodian's AstraZeneca issued computer (desktop and/or laptop) and in the Custodian's allocated personal storage space(s); and emails maintained in the Custodian's mailbox in AstraZeneca's Office 365 environment as well as the Custodian's email archives (if applicable).

ii. Procter & Gamble defines "Custodial File" Documents, if any, maintained in the Custodian's hard copy files, on the Custodian's issued computer, in the Custodian's allocated personal storage space, or in the Custodian's email mailbox.

iii. Pfizer defines "Custodial File" to include: (i) hard copy files that can be reasonably identified as belonging to the Custodian; (ii) documents on the personal computer hard drive(s) used by the Custodian while employed by Pfizer; (iii) e-mail and attached documents, including centralized e-mail storage, from the Custodian's e-mail account(s) provided by Pfizer, including email archives.

iv. Wyeth defines "Custodial File" to include: (i) hard copy files that can be reasonably identified as belonging to the Custodian; (ii) documents on the personal computer hard drive(s) used by the Custodian while employed by Pfizer; (iii) e-mail and attached documents, including centralized e-mail storage, from the Custodian's e-mail account(s) provided by Pfizer, including email archives.

B. ELECTRONICALLY STORED INFORMATION

1. Production in Reasonably Usable Form

a. Without waiving any available objection to any request for production, the Parties shall produce ESI in reasonably usable form. Except for Documents produced in native format as agreed herein or as agreed hereafter by the Parties, such reasonably usable form shall be the single-page TIFF-image format with extracted or OCR text and available metadata as set out in Attachment A (defined as "TIFF-Plus format"), which is incorporated in full in this Protocol. Notwithstanding the foregoing, the Receiving Party, for good cause explained in the request, may request native format versions of specifically identified ESI produced originally in TIFF-Plus format. Provided that the requests: (1) are reasonable in volume; (2) specifically identify by Bates number the ESI produced originally in TIFF format; and (3) seek files that are not redacted or otherwise cannot be produced in their native form, the Producing Party shall respond in good faith to-such requests. The Parties will negotiate in good faith regarding the Requesting Party's reproduction request and whether cost shifting is appropriate. At its discretion, the Producing Party may produce certain Documents in native form with slipsheets in the format set forth in Appendix A, Paragraph A.15

b. Redactions. As set forth in the governing Protective Order, the Producing Party may redact from any TIFF image, metadata field, or native file material that is protected from disclosure by applicable privilege or immunity, that is governed by the EU Data Privacy Directive or other applicable privacy law or regulation, private personal information of employees or other persons; commercially sensitive or proprietary non-responsive information, or other information that the Protective Order entered allows to be redacted.

The Producing Party shall identify redactions clearly on the face of any *.tif image, either with "Redacted" or the redaction

reason on the face of the Document if space allows. (e.g.: Privilege, Voluntary Reporter). In lieu of a redaction log, the Producing Party may provide a metadata field in the .dat file that identifies the type(s) of redactions that appear on a Document (e.g. Attorney Client, Work Product, etc.).

c. Each Party may make reasonable requests, for good cause, for production of specifically identified Documents in color. The Parties shall confer whether cost shifting is appropriate.

2. Electronic Spreadsheets, PowerPoint, Word, SAS, PDF, and Multimedia Files

Electronic spreadsheets (e.g., Excel), Powerpoints, Word, PDF, SAS, and Multimedia Files shall be produced in native format, unless they are authorized to be redacted. Plaintiffs shall meet and confer with individual Defendants with respect to the format of production for redacted documents.

After such redactions, the Producing Party either shall produce the redacted Document in the reasonably usable form set out in Attachment A, or shall produce the redacted copy in native format.[3] Certain types of files, such as system, program, and sound files, will not be amenable to conversion into anything meaningful in *.tif format. Relevant files that cannot be provided in a meaningful *.tif format will be produced in native form with a *.tif slip sheet. Examples of file types that may not convert include but are not limited to file types with the following extensions:

*.exp *.ilk *.res *.trg *.tlh *.idb *.pdb *.pch *.opt *.lib
*.cab *.mov *.mp3 *.swf *.psp *.chi *.chm *.com *.dll
*.exe *.hlp *.ivi *.ivt *.ix *.msi *.nls *.obj *.ocs *.rmi
*.sys *.tmp *.tff *.vgx *.wav *.wpg *.iso *.pdb *.eps
*.mpeg *.mpg *.ram *.rm *.psd *.ai *.aif *.bin *.hqx
*.snd *.mpe *.wmv *.wma *.xfd *.db *.xml

3. Structured Data from Enterprise Databases and Database Management Systems

The Parties shall meet and confer regarding production format of any structured data and/or non-standard data requests. The Parties will work to

[3] AstraZeneca will natively redact Excel files and produce in native form. Similarly, should AstraZeneca produce SAS files, such files will be produced in native format with the exception that SAS or comparable files requiring redaction will be converted to CSV or Excel format to allow for native redaction and produced in such format.

identify an appropriate format that will allow the Requesting Party to use and search the data in a meaningful way, such as an already existing and reasonably available report, or an export from the original database of discoverable information in a format compatible with Microsoft Excel or Microsoft Access produced in native format. A Producing Party shall neither be obligated to create and/or produce a copy of a database, nor provide another Party with access to a database.

Structured data from database and database management systems that has already been collected and or produced in other litigations or for some other purpose as of the date of this Order, shall be acceptable in the form collected or produced.

The Receiving Party shall not be precluded from seeking production in a different format; the Parties shall meet and confer in good faith whether cost shifting is appropriate.

4. Additional Procedures for Native Format Files

a. Procedures for assigning production numbers and confidentiality information to files produced in native format are addressed in Appendix A, Paragraph A.15.

b. Any Party seeking to use, in any proceeding in this Litigation, files produced in native format shall do so subject to the following:

i. If the native file has been converted to TIFF-image or hardcopy, the original production number and confidentiality designation shall be stamped on each page of the resulting TIFF-image or hardcopy document representing the original native-format file, with a suffix added to the production number to identify the particular page in the file *(e.g.,* XYZ00001_001). In addition, the MD5 or SHA-1 hash value of the native file from which the TIFF-image or hardcopy document was generated shall be placed on, at a minimum, the first page of the TIFF-image or hardcopy document.

ii. If the file will be used in its native format, the Party seeking to use the native file shall create and attach thereto a slip sheet which provides the production number and MD5 hash value of the file as well as any confidentiality designation.

iii. Any Party using native format files for any reason during the course of the Litigation, for instance as an exhibit at a

deposition or at trial, as an exhibit for a motion, or Documents given to any experts or consultants, is responsible for ensuring that the slip sheet associated with each native file is prepended to the file prior to its use. Use of a file in native format, or use of a TIFF image or hardcopy document representing the original native-format file, shall constitute a representation that the file being used is an accurate, unaltered and complete depiction of the original native-format file.[4]

5. Use of Search Filters

a. Date Range. The Parties shall meet and confer regarding the appropriate date range to be applied to each Custodial File and Non-Custodial Document Source. The Parties shall meet and confer on the date cut off to be applied.

b. To contain costs in the identification of non-duplicative relevant ESI for review and production, the Parties may wish to use advanced search and retrieval technologies, including email threading, predictive coding or other technology-assisted review. The Producing Party shall meet and confer with the Requesting Party to discuss search and retrieval method(s) the Producing Party has determined to apply to its Sources. If changes to such methods are deemed necessary by the Producing Party, the Producing Party will so notify the Requesting Party and the Parties shall meet and confer regarding proposed changes if the Requesting Party does not agree to them.

c. Each Defendant will propose a list of search terms to Plaintiffs within 30 days of entry of this Order. Plaintiffs will meet and confer with the Defendant regarding those terms within 30 days of Defendant's proposal. Agreement on search terms will be completed promptly, but such agreement will not itself prevent Plaintiffs from reasonable requests for additional search terms, subject to a Defendant's agreement or the Court's intervention, throughout the course of discovery as limited by the deadlines set forth in a Discovery Scheduling Order to be agreed upon by the Parties.

d. The fact that any electronic file has been identified in agreed-upon searches shall not prevent the Producing Party from withholding such file from production pursuant to the terms of

[4] E-mail produced by AstraZeneca with reflect an HTML rendering of the MSG format.

the Protective Order or as required by the EU Data Privacy Directive.

e. Nothing in this section shall limit a Party's right to reasonably seek agreement from the other Parties or a Court ruling to modify previously agreed-upon search terms, later requests for search term validation, or procedures for advanced search and retrieval technologies.

6. Collection and Deduplication

The Parties shall apply standard De-NISTing filters in order to exclude irrelevant, non-substantive files from hosting, review and production.

7. To manage the costs associated with review, production, and storage costs of duplicative Documents for both Plaintiffs and Defendants, the Parties shall confer regarding the deduplication to be applied. . The Parties agree that a Producing Party may employ either Source level (*i.e.*, deduped within a Source) or global deduplication of Documents *(i.e.,* both within a particular Source and across all Sources).[5, 6] "Duplicate ESI" means files that are exact duplicates based on the files' MD5 or SHA-1 hash values. The Producing Party need produce only a single copy of responsive Duplicate ESI. Entire Document families may constitute Duplicate ESI. De-duplication shall not break apart families. When the Producing Party employs global deduplication and the same Duplicate ESI exists in multiple Sources, those Sources shall be listed in the Global Source field identified in Paragraph A.14.(c) of Attachment A.

8. Production Rules

Due to the contextual relationship of ESI, the Parties will maintain family relationships for electronic data; non-relevant attachments may be excluded from production. The Parties will make relevancy and production determinations for hard copy documents at the Document level.

9. Prioritization

The Parties agree to meet and confer regarding prioritizing collection and production efforts of relevant Document Sources. Documents will be produced on a rolling basis pursuant to a schedule agreed upon by the Parties and

[5] There may be Non-Custodial Document Sources that cannot be globally deduped or for which global deduplication is not appropriate. Accordingly, the Producing Party will not employ global deduplication for such sources.

consistent with the Case Management Order. The Parties reserve the right to supplement production as necessary.

C. DOCUMENTS THAT EXIST ONLY IN HARDCOPY (PAPER) FORM

A Party shall produce Documents that exist in the normal course of business only in hardcopy form in scanned electronic format, redacted as necessary, in accordance with the procedures set out in Attachment A. The scanning of original hardcopy documents does not otherwise require that the scanned images be treated as ESI.

IT IS SO ORDERED.
DATED: May 9, 2017

Digitally signed by Judge David R. Herndon
Date: 2017.05.09 15:33:04 -05'00'

UNITED STATES DISTRICT JUDGE

ATTACHMENT A

A.1. Image Files

Documents produced in *.tif format will be single page black and white *.tif images at 300 DPI, Group IV compression. To the extent possible, original orientation will be maintained *(i.e.,* portrait-to-portrait and landscape-to-landscape). Each *.tif image will be assigned a unique name matching the production number of the corresponding page. Such files will be grouped in folders of no more than 1,000 *.tif files each unless necessary to prevent a file from splitting across folders. Files will not be split across folders and separate folders will not be created for each file. Production ("Bates") numbers shall be endorsed on the lower right corner of all images. This number shall be a unique, consistently formatted identifier that will:

a) be consistent across the production;

b) contain no special characters; and

c) be numerically sequential within a given file.

Bates numbers should be a combination of an alpha prefix along with an 8 digit number (e.g. ABC-00000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions. Confidentiality designations, if any, will be endorsed on the lower left corner of all images and shall not obscure any portion of the original file.

A.2. File Text

Except where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, full extracted text will be provided in the format of a single *.txt file for each file *(i.e.,* not one *.txt file per *.tif image). Where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, the redacted *.tif image will be OCR'd and file-level OCR text will be provided in lieu of extracted text. If redacted Documents are embedded within a parent Document, the parent Document will be produced in TIFF format with Document level OCR text.

Searchable text will be produced as Document-level multi-page UTF-8 text files with the text file named to match the beginning production number of the Document. The full path of the text file must be provided in the *.dat data load file.

A.3. *.tifs of Redacted ESI

*.tifs of redacted ESI shall convey the same information and image as the original document, to the extent possible and available, including all non-redacted elements and formatting which are visible in any view of the document in its native application (i.e. track changes). Each redacted area shall bear a label containing the reason for the redaction if space allows per B.1.b of the Protocol.

A.4. Redactions

For ESI that is redacted, all metadata fields listed in A.14 will be provided in the .dat file and will include all non-redacted metadata. Metadata may be redacted as appropriate pursuant to Protective Order and this Protocol. Redacted documents shall be identified as such in the load file provided with the production as required in A.14. A Document's status as redacted does not relieve the Producing Party from providing the metadata required herein.

A.5. Spreadsheet or Worksheet Files

To the extent that spreadsheet files, including without limitation Microsoft Excel files (*.xls or *.xlsx), are redacted and therefore produced in *.tif image format, such *.tif images will display hidden rows, columns, and worksheets, if any, in such files to the extent available. If redactions can be made natively, then the native redacted spreadsheet shall be produced.

A.6. Parent-Child Relationships

Parent-child relationships *(e.g.,* the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the .dat load file pursuant to paragraph A.14 below.

Because the relationship between hard copy documents is artificial, the Parties will treat each hard copy document as independent subject to Paragraph A.12 below.

A.7. Dynamic Fields

Documents containing dynamic fields such as file names, dates, and times will be produced showing the field type (e.g., "[FILENAME]" or "[AUTODATE]"), when in *.tif format, rather than the values for such fields existing at the time the file is processed.

A.8. English Language

To the extent any data exists in more than one language, the data will be produced in English, if available. If no English version of a file is available, the Producing Party shall not have an obligation to produce an English translation of the data.

In effort to manage costs, for the purpose of producing Documents under this Order in response to discovery requests, the Parties agree that they will utilize translation software only for internal review of Documents identified as potentially privileged by application of the Producing Party's privilege filter. Defendants do not intend to waive privilege or designations of Confidential Discovery Material or Confidential Personal Information, as defined in the Protective Order for inadvertent production of such information. Any and all Documents produced containing foreign language remain subject to and are governed by the terms of the Protective Order.

A.9. Embedded Objects

Some Microsoft Office and .RTF files may contain embedded objects. Such objects typically are the following file types: Microsoft Excel, Word, PowerPoint, Project, Outlook, and Access; and PDF. Subject to claims of privilege and immunity, as applicable, objects with those identified file types shall be extracted as separate files and shall be produced as attachments to the file in which they were embedded. If embedded objects are privileged or require redaction, the parent Document will be produced in *.tif format with Document level OCR text. If such embedded objects are merely non-substantive graphic files such as corporate logos, such embedded objects need not be produced as separate Documents as their content is visible in the parent Document.

A.10. Compressed Files

Compressed file types (i.e., .CAB, .GZ, .TAR. .Z, .ZIP) shall be decompressed. All files that exist within the compressed containers will be extracted to individual files. If compressed container files are found within compressed container files those files should be further decompressed and extracted to individual files.

A.11. Encrypted or Corrupt Files

The Producing Party will take reasonable steps, prior to production, to unencrypt or restore any discoverable ESI that is encrypted *(e.g.*, password-protected) or corrupt, and will produce relevant, non-privileged Documents that can be reasonably unencrypted or restored.

A.12. Scanned Hardcopy Documents

a) In scanning hardcopy documents, multiple distinct documents should not be merged into a single record, and single documents should not be split into multiple records *(i.e.*, hard copy documents should be logically unitized).

b) For scanned images of hard copy documents, OCR should be performed on a Document level and provided in Document-level *.txt files named to match the production number of the first page of the Document to which the OCR text corresponds. OCR text should not be delivered in the data load file or any other delimited text file.

c) In the case of an organized compilation of separate hardcopy documents—for example, a binder containing several separate documents behind numbered tabs—the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the family fields set out below.

A.13. Production Numbering

In following the requirements of Paragraph A.1, the Producing Party shall take reasonable steps to ensure that attachments to Documents are assigned production numbers that directly follow the production numbers on the Documents or files to which they were attached. If a production number or set of production numbers is skipped, the skipped

number or set of numbers will be noted. In addition, wherever possible, each *.tif image will have its assigned production number electronically "burned" onto the image.

A.14. Data and Image Load Files

a) Load Files Required. Unless otherwise agreed, each production will include a data load file in Concordance (*.dat) format and an image load file in Opticon (*.opt) format.

b) Load File Formats.

i. Load file names should contain the volume name of the production media. Additional descriptive information may be provided after the volume name. For example, both ABC001.dat or ABC001 metadata.dat would be acceptable.

ii. Unless other delimiters are specified, any fielded data provided in a load file should use Concordance default delimiters. Semicolon (;) should be used as multi-entry separator.

iii. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.

c) Fields to be Included in Data Load File. For all Documents produced, the following metadata fields for each Document, if available at the time of collection and processing and unless such metadata fields are protected from disclosure by attorney-client privilege or work-product immunity or otherwise prohibited from disclosure by law or regulation, including the EU Data Privacy Regulation, will be provided in the data load file pursuant to subparagraph (a) above, except to the extent that a Document has been produced with redactions. The term "Scanned Docs" refers to documents that are in hard copy form at the time of collection and have been scanned into *.tif images. The term "Email and E-Docs" refers to files that are in electronic form at the time of their collection.

The Parties shall meet and confer regarding any metadata fields sought beyond those listed below.

Field*	Sample Data	Scanned Docs	Email and E-Docs	Comment
PRODBEG	ABC00000001	Yes	Yes	Beginning production number
PRODEND	ABC00000008	Yes	Yes	Ending production number

PRODBEGATT	ABC00000009	Yes	Yes	Beginning production number of parent in a family
PRODENDATT	ABC00001005	Yes	Yes	Ending production number of last page of the last attachment in a family
ATTACH	Attach1.doc; Attach2.doc	No	Yes	Filenames of all attached records, separated by semi-colons
NUMATTACH	2	No	Yes	Total number of records attached to the document (value will always be 0 for the actual document)
CUSTODIAN/SOURCE	Smith, John	Yes	Yes	Name of Custodian/Source that possessed the Document
GLOBAL SOURCE (or ALL CUSTODIAN)	Doe, Jane; Jones, James	No	Yes	Custodian(s)/Source(s) that possess duplicate copies of the Document
NATIVEFILE	Natives\\\ 00000001.xls	N/A	Yes	Path and file name for native file on production media
DOCTYPE	Microsoft Office 2007 Document	N/A	Yes	Description of the type file for the produced record.
FILEPATH	\My Documents\ Document1.doc	N/A	Yes	Original source filepath for the record produced.
ALLFILEPATHS (Produced if Party globally dedups)		N/A	Yes	Paths to duplicate maintained by other Custodians/Sources
FILENAME	Document1.doc	N/A	Yes	Name of original electronic file as collected.
DOCEXT	DOC	N/A	Yes	File extension for email or e-doc
DOC TYPE	Email	N/A	Yes	Type of document

PAGES	2	Yes	Yes	Number of pages in the produced Document (not applicable to native file productions).
FILE SIZE		N/A	Yes	File size
AUTHOR	John Smith	N/A	Yes	Author information as derived from the properties of the Document.
DATECREATED	10/09/2005	N/A	Yes	Date that non-email file was created as extracted from file system metadata
DATELASTMOD	10/09/2005	N/A	Yes	Date that non-email file was modified as extracted from file system metadata
DOCTITLE	Meeting Minutes	N/A	Yes	"Title" field extracted from metadata properties of the Document
SUBJECT	Changes to Access Database	N/A	Yes	"Subject" field extracted from email message
FROM	John Beech	N/A	Yes	"From" field extracted from email message
TO	Janice Birch	N/A	Yes	"To" field extracted from email message
CC	Frank Maple	N/A	Yes	"Cc" or "carbon copy" field extracted from email
BCC	John Oakwood	N/A	Yes	"Bcc" or "blind carbon copy" field extracted from email message
DATESENT	10/10/2005	N/A	Yes	Sent date of email message (mm/dd/yyyy format)
TIMESENT	18:33:00	N/A	Yes	Sent time of email message, time zone set to UTC
DATERCVD	10/10/2005	N/A	Yes	Received date of email message (mm/dd/yyyy format)

TIMERCVD	18:33:00	N/A	Yes	Received time of email message, time zone set to UTC
CONFIDENTIALITY	CONFIDENTIAL	Yes	Yes	Text of confidentiality designation, if any
TEXTPATH	Text\\\.txt	Yes	Yes	Path to *.txt file containing extracted or OCR text
PRODVOL	VOL001	Yes	Yes	Name of the Production Volume
REDACTED	Yes/No	Yes	Yes	Identifies whether a Document contains redactions
REDACTION TYPE	Privilege	Yes	Yes	Identifies the reason for a redaction.
MD5 (or SHAI) HASH VALUE	e4d909c290d0fb1ca068ffaddf22cbd0	N/A	Yes	Unique identifier

*Field designations are friendly names for ease of reference. Actual column names in load files may differ so long as the column names are consistent across the Producing Party's production and have the same meaning as the fields above.

A.15. Files Produced in Native Format

Any electronic file produced in native format shall be given a file name consisting of a unique Bates number and, as applicable, a confidentiality designation; for example, "ABC00000002 Confidential." For each native file produced, the production will include a *.tif image slipsheet indicating the production number of the native file and the confidentiality designation, and stating "File Produced Natively". To the extent that it is available, the original file text shall be provided in a Document-level multi-page UTF-8 text file with a text path provided in the *.dat file; otherwise the text contained on the slipsheet shall be provided in the *.txt file with the text path provided in the *.dat file.

A.16. Production Media

Unless otherwise agreed, Documents will be produced on optical media (CD/DVD), external hard drive, secure FTP site, or similar electronic format. Such media should have an alphanumeric volume name; if a hard drive contains multiple volumes, each volume should be contained in an appropriately named folder at the root of the drive. Volumes should be numbered consecutively (ABC001, ABC002, etc.). Deliverable media should be labeled with the name of this action, the identity of the Producing Party, and the following information: Volume name, production range(s), and date of delivery.

Each Defendant will provide one copy of its productions to Plaintiff's third party discovery vendor. If a vendor has not been retained, Defendants will provide the production to Plaintiff's designated representative upon condition that, upon selection of a vendor, Plaintiff's designated representative will provide any production(s) to its vendor that were directly produced to the designated representative. Anyone accessing a production agrees to be subject to the Protective Order, and must sign the Acknowledgement attached thereto.

A.17. Encryption of Production Media

To maximize the security of information in transit, any media on which Documents are produced may be encrypted by the Producing Party. In such cases, the Producing Party shall transmit the encryption key or password to the Requesting Party, under separate cover, contemporaneously with sending the encrypted media. The Receiving Parties in this matter are on notice that certain data produced may originate from Sources that originate in a jurisdiction outside the United States and are subject to the protection of foreign privacy and data protection laws such as the EU Data Privacy Directive, and the Receiving Parties therefore agree to follow the strictest security standards in guarding access to said data.